

Week commencing 31 August 2026

COVERAGE

17 – 30 August 2026

AUDIENCE

Technology and security leadership · platform and delivery leads

HANDLING

Internal use — not for onward distribution

IF YOU JUST REMEMBER ONE THING FROM THIS BRIEFING...

Patch windows have collapsed faster than most change boards can meet.

VMware's vCenter flaw went from patch to 361 compromised servers in nine days; Microsoft's SharePoint bypass was exploited hours after a public proof-of-concept. CISA added neither to its exploited-vulnerabilities catalogue until 18 August — after the damage. Ask your platform owner today: does emergency-patch authority for management-plane software beat the standard change window, or are we still waiting for KEV?

THIS FORTNIGHT

Platform change and AI regulation

PRIORITY

18 AUG

Four actively exploited flaws land in KEV catalogue at once

CISA added four flaws to its exploited-vulnerabilities catalogue on 18 August: SharePoint (CVE-2026-55040), VMware vCenter (CVE-2026-59310), Windows IKE (CVE-2026-33824) and macOS (CVE-2026-65400), all rated 9.1 or higher. The vCenter flaw alone compromised 361 servers across 47 countries within nine days of patch release.

So what: patch or isolate all four now; KEV addition trailed exploitation by days. Treat management-plane software as a same-day patch tier, not routine cycle.

PRIORITY

20 AUG

NCSC issues interim guidance for agentic AI after real incidents

NCSC published interim advice on 20 August for organisations building or operating agentic AI: sandbox agents, keep active human oversight, restrict access, log everything, and deny network connectivity by default. It follows incidents including a HuggingFace production breach in July driven end-to-end by an autonomous agent. Formal guidance follows later.

So what: agentic deployments need default-deny network egress before they need better prompts. Audit which production agents can currently reach the internet unrestricted.

PRIORITY

26 AUG

Azure OpenAI Assistants API retirement lands

Microsoft's Azure OpenAI Assistants API reached hard retirement on 26 August; calls to Assistants endpoints now fail outright. Foundry Agent Service (GA) is the replacement, though Foundry Agent Service classic itself retires 31 March 2027 — a second migration inside 18 months for anyone who moves there without checking.

So what: confirm which target you migrated to. Landing on Foundry Agent Service classic only defers the same problem to 2027.

WATCH

31 AUG

Bedrock's Claude Sonnet 5 promotional pricing expires today

AWS Bedrock's launch pricing for Claude Sonnet 5 — \$2/\$10 per million input/output tokens — expires 31 August, rising 50% to \$3/\$15 from 1 September. No migration path exists beyond absorbing the cost or re-benchmarking against Sonnet 4.6 or a cheaper GPT-5.6 tier.

So what: any workload sized against launch pricing now costs 50% more overnight. Recheck AI budget lines built on August-vintage estimates.

ACTION QUEUE

Changes to act on this fortnight

CHANGE	PLATFORM	WHAT IT BREAKS OR REQUIRES	ACT BY
CVE-2026-55040 SharePoint bypass	Microsoft SharePoint	Unauthenticated JWT forgery, admin impersonation; exploited within hours of PoC.	Immediate
CVE-2026-59310 vCenter traversal	Broadcom VMware	Reverse-SSH persistence; 361 servers already compromised worldwide.	Immediate
Assistants API hard retirement	Microsoft Azure	Assistants endpoints now return errors — confirm migration to Foundry Agent Service (GA).	Immediate
Interim agentic AI guidance	Cross-platform / AI agents	Sandbox, restrict access, log, and deny-by-default network egress for agents.	Before next edition
Sonnet 5 launch pricing ends	AWS Bedrock	Token cost rises 50% from 1 September — rebudget affected workloads.	1 Sep

Identifiers and dates as published by CISA, Microsoft, AWS and NCSC. Confirm applicability against your own estate before scheduling.

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- AI Act Annex III high-risk obligations apply since 2 August; the AI Office is running compliance dialogues with GPAI providers.
- NCSC’s interim agentic-AI guidance — sandboxing, oversight, default-deny networking — is live from 20 August pending formal standards.

Approaching

- Entra ID SSPR accepts only pre-registered authentication methods from 7 September — audit registered methods now.
- ICO’s automated-decision-making guidance consultation opens August 2026; final guidance due winter — early input shapes procurement asks.

Standing watch — sovereign AI processing. Microsoft’s Copilot Interactions in-country processing expands to 15 European countries by end of 2026; Anthropic and OpenAI still have no dedicated EU inference region. No change this fortnight.

RECOMMENDED

Three things to do before the next edition

- Patch or isolate SharePoint, vCenter and Windows IKE this week; don’t wait for KEV confirmation.
- Audit production AI agents for default-deny network egress against NCSC’s interim guidance.
- Confirm Assistants API migration landed on GA Foundry Agent Service, not the classic tier.

OUTLOOK — NEXT FORTNIGHT

We assess it is highly likely CISA adds further identity or management-plane CVEs to KEV before the next edition. It is a realistic possibility that NCSC’s interim agentic guidance hardens into formal standards within the fortnight, and likely that AI inference pricing steps up further as promotional rates expire.

NEXT EDITION

Monday 14 September 2026. Send additions, corrections or platform intelligence to your ClearPath engagement lead.

